# AMENDMENT TRANSMITTAL LETTER

| Docket No. 41828875SUS |
|---|

| Application No. | Filing Date | Examiner | Art Unit |
|---|---|---|---|
| 09/652,360-Conf. #4462 | August 31, 2000 | A. Widhalm | 2152 |

Applicant(s): Wong et al.

Invention: METHODS AND SYSTEMS FOR SELECTING METHODOLOGY FOR AUTHENTICATING COMPUTER SYSTEMS ON A PER COMPUTER SYSTEM OR PER USER BASIS

**TO THE COMMISSIONER FOR PATENTS**

Transmitted herewith is an amendment in the above-identified application.

The fee has been calculated and is transmitted as shown below.

| CLAIMS AS AMENDED | | | | | |
|---|---|---|---|---|---|
| | Claims Remaining After Amendment | Highest Number Previously Paid | | Number Extra Claims Present | Rate | |
| Total Claims | 21 | - 27 | = | | x | |
| Independent Claims | 3 | - 4 | = | | x | |
| Multiple Dependent Claims (check if applicable) ☐ | | | | | | |
| Other fee (please specify): Extension for response within first month | | | | | | 120.00 |
| TOTAL ADDITIONAL FEE FOR THIS AMENDMENT: | | | | | | 120.00 |

☒ Large Entity ☐ Small Entity

☐ No additional fee is required for this amendment.

☒ Please charge EFT Account No SEA1PIRM in the amount of $ 120.00 .

☐ A check in the amount of $ 120.00 to cover the filing fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized to charge and credit Deposit Account No. 50-0665 as described below.

☒ Credit any overpayment.

☒ Charge any additional filing or application processing fees required under 37 CFR 1.16 and 1.17.

Maurice J. Pirio

Dated: August 17, 2007

Maurice J. Pirio
Attorney/Agent Reg. No.: 33,273

PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8000

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: Aug 17, 2007 Signature: Joyce Valentine (Joyce Valentine)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Wong et al.

Application No.: 09/652,360 | Confirmation No.: 4462

Filed: August 31, 2000 | Art Unit: 2152

For: METHODS AND SYSTEMS FOR SELECTING METHODOLOGY FOR AUTHENTICATING COMPUTER SYSTEMS ON A PER COMPUTER SYSTEM OR PER USER BASIS | Examiner: A. Widhalm

**AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION**

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

## INTRODUCTORY COMMENTS

In response to the Office Action dated April 17, 2007, please amend the above-identified U.S. patent application as follows:

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks/Arguments** begin on page 8 of this paper.

AMENDMENTS TO THE CLAIMS.

1-29. (Canceled)

30. (Currently Amended) A method in a server computer of authenticating client computer systems using various authentication mechanisms, each authentication mechanism specifying a type of information necessary to verify a purported identity of a client computer system, each client computer system having client-specific knowledge of the information necessary to verify the purported identity of the client computer system, the method comprising:

storing, for each of the client computer systems, an indication of an authentication mechanism that can be used to authenticate the client computer system, at least some client computer systems having multiple authentication mechanisms that can be used to authenticate the client computer system, the indications being stored based on receiving from a controlling client computer system a plurality of ~~an~~ instructions, each instruction identifying a client computer system and identifying at least one ~~that indicates an~~ authentication ~~methodology~~ mechanism that ~~is to~~ can be used to authenticate ~~a~~ the client computer system, ~~that is~~ each client computer system being a separate computer system from the controlling client computer system, the authentication ~~methodology~~ mechanism being selected from multiple authentication ~~methodologies~~ mechanisms based on authentication abilities indicating authentication ~~methodologies~~ mechanisms that the client computer system supports and access rights of the client computer system to access resources;

after receiving ~~the~~ an instruction for a client computer system and before authenticating ~~the~~ that client computer system, receiving a request from ~~the~~ that client computer system to access a service of the server computer

system, the request including a purported identity of that client computer system; and

upon receiving the request from the that client computer system to access a service of the server computer, when that client computer system can be authenticated using multiple authentication mechanisms, selecting an authentication mechanism and initially authenticating the that client computer system using the indicated selected authentication methodologymechanism based on the information necessary to verify the purported identity of that client computer system.

31. (Currently Amended) The method of claim 30 wherein the at least one of the plurality of instructions indicates that multiple authentication methodologies mechanisms can be used to authenticate the a client computer system and wherein the that client computer system is authenticated using one of the indicated authentication methodologiesmechanisms.

32. (Currently Amended) The method of claim 30 wherein the plurality of instructions indicates that the same authentication methodology mechanism is to be used to authenticate multiple client computer systems and wherein the multiple client computer systems are authenticated using the indicated authentication methodologymechanism.

33. (Currently Amended) The method of claim 30 wherein the plurality of instructions indicates that multiple authentication methodologies mechanisms can be used to authenticate multiple client computer systems and wherein the multiple client computer systems are authenticated using one of the indicated authentication methodologiesmechanisms.

34. (Currently Amended) The method of claim 30 wherein one of the multiple authentication methodology mechanisms is an assertion authentication.

35. (Currently Amended) The method of claim 30 wherein one of the multiple authentication ~~methodology~~ mechanisms is a basic HTTP authentication.

36. (Currently Amended) The method of claim 30 wherein one of the multiple authentication ~~methodology~~ mechanisms is digest authentication.

37. (Currently Amended) The method of claim 30 wherein one of the multiple authentication ~~methodology~~ mechanisms is an NTLM authentication.

38. (Currently Amended) A method in a controlling client computer system for providing indications of authentication ~~methodologies~~ mechanisms to a server computer system, each authentication mechanism specifying a type of information necessary to verify a purported identity of a client computer system, each client computer system having client-specific knowledge of the information necessary to verify the purported identity of the client computer system, the method comprising:

generating ~~an~~ a plurality of instructions, each instruction identifying a client computer system and identifying at least one ~~that indicates an authentication methodology~~ mechanism that ~~is~~ can be used to authenticate a the client computer system, each client computer system being ~~that is~~ a separate computer system from the controlling client computer system, the authentication ~~methodology~~ mechanism being selected from multiple authentication ~~methodologies~~ mechanisms based on authentication abilities indicating authentication ~~methodologies~~ mechanisms that the client computer system supports and access rights of the client computer system to access resources; and

sending the generated instructions to the server computer system so that upon receiving a request from ~~the~~ a client computer system to access a service of the server computer system, the request including a purported identity of that client computer system, after the instruction is received at the server

computer system and before authenticating ~~the~~ that client computer system, when that client computer system can be authenticated using multiple authentication mechanisms, the server computer system ~~can~~ selects an authentication mechanism and initially authenticate ~~the~~ that client computer system using the ~~indicated~~ selected authentication ~~methodology~~mechanism based on the information necessary to verify the purported identity of that client computer system.

39. (Currently Amended) The method of claim 38 wherein ~~the~~ at least one of the plurality of instructions indicates that multiple authentication ~~methodologies~~ mechanisms can be used to authenticate ~~the~~ a client computer system and wherein ~~the~~ that client computer system is authenticated by the server computer system using one of the indicated authentication ~~methodologies~~mechanisms.

40. (Currently Amended) The method of claim 38 wherein the plurality of instructions indicates that the same authentication ~~methodology~~ mechanism is to be used to authenticate multiple client computer systems and wherein the multiple client computer systems are authenticated by the server computer system using the indicated authentication ~~methodology~~mechanism.

41. (Currently Amended) The method of claim 38 wherein the plurality of instructions indicates that multiple authentication ~~methodologies~~ mechanisms can be used to authenticate multiple client computer systems and wherein the multiple client computer systems are authenticated by the server computer system using one of the indicated authentication ~~methodologies~~mechanisms.

42. (Currently Amended) The method of claim 38 wherein one of the multiple authentication ~~methodology~~ mechanisms is an assertion authentication.

43. (Currently Amended) The method of claim 38 wherein one of the multiple authentication ~~methodology~~ mechanisms is a basic HTTP authentication.

44. (Currently Amended) The method of claim 38 wherein one of the multiple authentication ~~methodology~~ mechanisms is digest authentication.

45. (Currently Amended) The method of claim 38 wherein one of the multiple authentication ~~methodology~~ mechanisms is an NTLM authentication.

46. (Currently Amended) A tangible computer-readable medium containing instructions for controlling a server computer system to authenticate entities using various authentication mechanisms, each authentication mechanism specifying a type of information necessary to verify a purported identity of an entity, each entity having entity-specific knowledge of the information necessary to verify the purported identity of the entity, by a method comprising:

storing for each of the entities an indication of an authentication mechanism that can be used to authenticate the entity, at least some entities having multiple authentication mechanisms that can be used to authenticate the entity, the indications being stored based on receiving from a controlling entity an ~~a~~ plurality of instructions, each instruction identifying an entity and identifying at least one ~~that indicates an authentication methodology~~ mechanism that is to can be used to authenticate an the entity, the authentication ~~methodology~~ mechanism being selected from multiple authentication ~~methodologies~~ mechanisms based on authentication abilities of the entity that indicate which authentication ~~methodologies~~ mechanisms are supported by the entity, the controlling entity being a separate entity from the each entity;

after receiving the an instruction from the controlling entity for an entity and before authenticating the ~~client computer system~~ that entity, receiving a request from

~~the~~ that entity to access a service of the server computer system, the request including a purported identity of that entity; and

upon receiving the request from ~~the~~ that entity to access a service of the server computer system, when that entity can be authenticated using multiple authentication mechanisms, selecting an authentication mechanism and initially authenticating ~~the~~ that entity using the ~~indicated~~ selected authentication ~~methodology~~mechanism based on the information necessary to verify the purported identity of that entity.

47. (Currently Amended) The computer-readable medium of claim 46 wherein at least one of the plurality of ~~the~~ instructions indicates that multiple authentication ~~methodologies~~ mechanisms can be used to authenticate ~~the~~ an entity and wherein ~~the~~ that entity is authenticated using one of the indicated authentication ~~methodologies~~mechanisms.

48. (Currently Amended) The computer-readable medium of claim 46 wherein the plurality of instructions indicates that the same authentication ~~methodology~~ mechanism is to be used to authenticate multiple entities and wherein the multiple entities are authenticated using the indicated authentication ~~methodology~~mechanism.

49. (Currently Amended) The computer-readable medium of claim 46 wherein the plurality of instructions indicates that multiple authentication ~~methodologies~~ mechanisms can be used to authenticate multiple entities and wherein the multiple entities are authenticated using one of the indicated authentication ~~methodologies~~mechanisms.

50. (Currently Amended) The computer-readable medium of claim 49 wherein the authentication ~~methodology~~ mechanism is selected from a group consisting of an assertion authentication, a basic HTTP authentication, a digest authentication, and an NTLM authentication.

## REMARKS

Claims 30-50 are pending in this application. Claims 30-50 are amended.

Applicant would like to thank the Examiner for the courtesy extended during the telephonic interview on June 20, 2007. During the interview, the Examiner and applicant's representative discussed proposed claim amendments to overcome the cited art. Applicant's representative indicated that applicant would submit amended claims to further clarify the subject matter of the invention.

The Examiner has rejected claims 30-33, 35, 38-41, 43, and 46-49 under 35 U.S.C. § 103(a) over Shambroom and Wood; and has rejected claims 34, 36-37, 42, 44-45, and 50 under 35 U.S.C. § 103(a) over Shambroom, Wood, and Applicant Admitted Prior Art. Applicant respectfully traverses these rejections.

Applicant has amended the pending claims to clarify (1) that applicant's authentication mechanism specifies "a type of information necessary to verify a purported identity of a client computer system" or "entity," and (2) that at least some client computer systems or entities have "multiple authentication mechanisms that can be used to authenticate the client computer system" or "entity." As amended, claims 30-45 recite "each authentication mechanism specifying a type of information necessary to verify a purported identity of a client computer system." As amended, claims 30-37 also recite "at least some client computer systems having multiple authentication mechanisms that can be used to authenticate the client computer system." As amended, claims 38-45 also recite "when the client computer system can be authenticated using multiple authentication mechanisms." As amended, claims 46-50 recite "each authentication mechanism specifying a type of information necessary to verify a purported identity of an entity" and "at least some entities having multiple authentication mechanisms that can be used to authenticate the entity."

Neither Shambroom nor Wood discloses or suggests an authentication mechanism that specifies "a type of information necessary to verify a purported identity of a client computer system" or "entity." Shambroom describes a key distribution center that sends

authentication information to a network server for authenticating a client. (See 8:27-44; Figure 3.) Shambroom simply describes sending authentication information, which is distinct from applicant's authentication mechanism that specifies a type of information. Under applicant's techniques, before any authentication information itself is sent from a client computer system or entity to the server, a separate controlling client computer system or entity identifies at least one authentication mechanism for the client computer system or entity; the authentication mechanism specifies a type of information that the client computer system or entity will be required to provide the server for authentication. This is distinct from sending authentication information itself. At most, Shambroom describes sending authentication information itself, applicant can find nothing in Shambroom that discloses or suggests an authentication mechanism that specifies "a type of information necessary to verify a purported identity of a client computer system" or "entity."

Nor can applicant find anything in Wood that discloses or suggests an authentication mechanism that specifies "a type of information necessary to verify a purported identity of a client computer system" or "entity." Indeed, the Examiner has only relied on Wood as teaching an "authentication methodology being selected from multiple authentication methodologies based on authentication abilities indicating authentication methodologies that the client computer supports and access rights of the client computer system to access resources." (Office Action, Apr. 17, 2007, p. 4.)

Further, Shambroom does not disclose or suggest that at least some client computer systems or entities have "multiple authentication mechanisms that can be used to authenticate the client computer system" or "entity." While Shambroom describes that another secure authentication protocol may be used, it recommends using an authentication protocol that incorporates the use of timestamps. (See 8:5-17.) Applicant can find nothing in Shambroom that discloses or suggests that more than one authentication protocol can be used to authenticate a particular client; the method described by Shambroom apparently selects one authentication protocol at the outset and uses that protocol to authenticate all clients. Applicant can find nothing in Shambroom that

discloses or suggests that at least some client computer systems or entities have "multiple authentication mechanisms that can be used to authenticate the client computer system" or "entity."

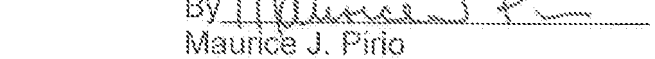
The Examiner believes that Wood describes that at least some client computer systems or entities that have "multiple authentication mechanisms that can be used to authenticate the client computer system" or "entity." Nevertheless, Wood does not disclose or suggest a controlling client computer system that identifies such authentication mechanisms. Wood describes a server that provides an entity (i.e., client) with a list of possible authentication schemes; the entity selects an authentication scheme and provides the server with one or more credentials as necessary for authentication under the selected scheme. (*See* 11:34-41.)

In view of the above amendment and remarks, applicant believes the pending application is in condition for allowance and respectfully requests reconsideration. If the Examiner has any questions or believes a telephone conference would further expedite prosecution of this application, the Examiner is encouraged to call the undersigned at (206) 359-8548.

If additional fees are due, please charge our Deposit Account No. 50-0665, under Order No. 418268758US from which the undersigned is authorized to draw.

Dated: August 17, 2007

Respectfully submitted,

By 

Maurice J. Pirio
Registration No.: 33,273
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8548
(206) 359-9548 (Fax)
Attorney for Applicant